

Wisconsin Privacy Laws

General Privacy

Telephone records; obtaining, selling, or receiving without consent; Wis. Stat. § 100.525.

No person may obtain, without the customer's consent, a customer's telephone records that identify:

- The telephone numbers dialed by the customer.
- The telephone numbers of calls made to the customer.
- The time or duration of the calls.

A person who illegally obtains this information is guilty of a felony, and may be required to forfeit property used or intended to be used in committing the felony. Also, the court may require the violator to pay the person whose telephone records have been misappropriated the amount of actual losses incurred, or \$1,000, whichever is greater; and the amount of gain to the violator as a result of the violation.

Nondisclosure of information on receipts; Wis. Stat. § 134.74.

No person who is in the business of selling goods at retail or selling services and who accepts a credit card or a debit card for the purchase of goods or services may issue a credit card or debit card receipt, for that purchase, on which is printed more than 5 digits of the credit card or debit card number.

Disposal of records containing personal information; Wis. Stat. § 134.97.

No financial institution, investment company, medical business, or tax preparation business, may dispose of records containing personal information without shredding the record, erasing the information from the record, or otherwise destroying the information. No may use any personal information that was not properly destroyed without the consent of the individual who is the subject of the information.

Under this law, "personal information" includes data related to an individual's:

- Health condition that is not public knowledge.
- Accounts with a financial institution
- Federal, state or local tax returns.

The personal information protected by this law must be “personally identifiable” such that it is capable of being associated with a particular individual through one or more identifiers.

In addition to criminal and civil forfeiture penalties imposed by the state, an individual who suffers damages because a person violates this law may sue the violator to recover the damages.

Notaries; confidentiality; Wis. Stat. § 137.01 (5m).

A notary public shall keep confidential all documents and information contained in documents reviewed by the notary public while performing his or her duties and may release the documents or information to a 3rd person only with the written consent of the person who requested the notary services.

A notary public who violates this law is liable to the person who requested the notary services for any damages that person may have incurred as a result of the violation.

Contracts requiring prisoner access to personal information; Wis. Stat. §§ 301.029.

The Wisconsin department of corrections may not enter into contracts relating to prisoner employment that would require a prisoner to perform data entry or telemarketing and have access to a person’s credit or debit card numbers, checking or savings account numbers, or social security number.

Notice of unauthorized acquisition of personal information; Wis. Stat. § 895.507.

Whenever an entity that collects personal information in the ordinary course of its business becomes aware that an unauthorized person has acquired the personal information, the business shall notify the individuals whose personal information has been acquired.

This law applies to any entity that does business in Wisconsin including a state or local government organization, but does apply to:

- A business conducted solely by an individual, such as a sole proprietorship.
- A federally regulated financial institution, or a person that has a contract with a federally regulated financial institution, if the financial institution has a policy in place to handle the unauthorized acquisition of personal information
- A health care plan, health care clearing house, or a health care provider that transacts personal information electronically, if the plan, clearing house, or provider complies with federal law regulating unauthorized acquisition of personal information.

Personal information under this law means an individual's:

- Name.
- Driver's license or state identification number.
- Financial account number, including credit or debit account number or any security code access code or password that would permit access to an individual's financial account.
- DNA profile.
- Fingerprint, voice print, retina or iris image, or any other unique physical representation.

The fact that an entity has failed to comply with this law may be used as evidence in court to prove that the entity is liable for damages incurred by an individual whose identity has been misappropriated. There are no other penalties imposed by this law.